(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－279198
（P2002－279198A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｇ０６Ｆ　17/60	２４８	Ｇ０６Ｆ　17/60	２４８　３Ｅ０４０
Ｇ０７Ｄ　9/00	４３６	Ｇ０７Ｄ　9/00	４３６Ａ

審査請求　有　請求項の数18　ＯＬ　（全 16 頁）

(21)出願番号　特願2001－74578(P2001－74578)

(22)出願日　平成13年３月15日(2001.3.15)

(71)出願人　592052416
株式会社みずほコーポレート銀行
東京都千代田区丸の内１丁目３番３号
(72)発明者　藤本　真紀子
東京都千代田区大手町１丁目５番５号　株式会社富士銀行内
(74)代理人　100068755
弁理士　恩田　博宣　（外１名）

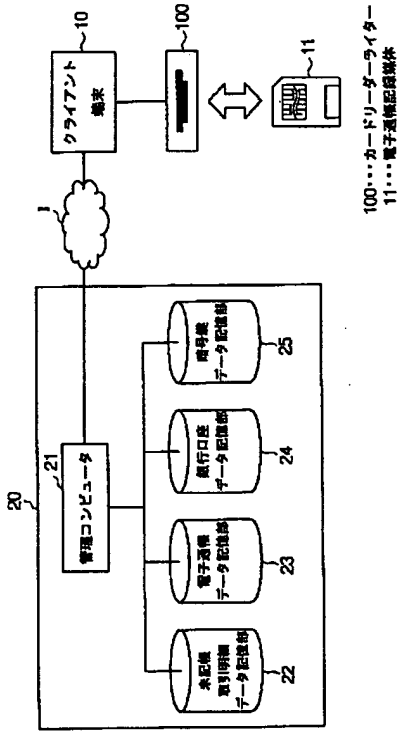
Ｆターム(参考)　3E040 AA07 BA01 BA06 BA16 BA18
CA12 CB10 DA10 EA02 EA10
FK08

(54)【発明の名称】　電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体

(57)【要約】

【課題】　利用者にとって効率的であり、金融機関にとっても確実に取引明細データを記録した電子通帳を提供することができる電子通帳記録方法、電子通帳登録システム及び電子通帳記録媒体を提供することにある。

【解決手段】　利用者は、クライアント端末１０を用いてユーザ認証を行った後で、電子通帳記録媒体１１に記録された媒体識別子１２１を電子通帳登録システム２０に送信する。管理コンピュータ２１は、受信した媒体識別子１２１と銀行口座に関するデータとから通帳識別子を生成する。さらに、管理コンピュータ２１は、この通帳識別子を銀行秘密鍵２５１で暗号化し、銀行署名データを生成する。そして、管理コンピュータ２１は、クライアント端末１０に通帳識別子と銀行署名データとを送信する。クライアント端末１０はこれらのデータを電子通帳記録媒体１１に記録する。これによって、銀行に認証された電子通帳記録媒体１１が生成される。



【特許請求の範囲】

【請求項１】　管理コンピュータを有する電子通帳登録システムを用いて、金融機関における取引明細データを記録媒体に記録する電子通帳記録方法であって、

前記管理コンピュータが、前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を受信し、電子通帳データ記憶手段に記録する第１の段階と、

前記管理コンピュータが、前記媒体識別子に基づいて金融機関秘密鍵で暗号化した金融機関署名データを生成する第２の段階と、

前記管理コンピュータが、前記金融機関署名データを前記記録媒体に記録するために出力する第３の段階とを有することを特徴とする電子通帳記録方法。

【請求項２】　前記電子通帳記録方法は、

前記管理コンピュータが、前記媒体識別子と金融機関口座識別子とに基づいて通帳識別子を生成し、前記電子通帳データ記憶手段に記録する段階をさらに有し、

前記第２の段階は、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、

前記第３の段階は、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを特徴とする請求項１に記載の電子通帳記録方法。

【請求項３】　前記電子通帳記録方法は、

前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合する段階と、

認証ができた場合には、前記管理コンピュータが前記記録媒体に記録する取引明細データを抽出する段階と、

前記管理コンピュータが、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力する段階とをさらに有することを特徴とする請求項１又は２に記載の電子通帳記録方法。

【請求項４】　前記電子通帳記録方法は、

前記管理コンピュータが、一方向関数を用いて前記取引明細データの一方向関数計算値を算出する段階と、

前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力する段階とをさらに有することを特徴とする請求項１～３のいずれか１項に記載の電子通帳記録方法。

【請求項５】　前記一方向関数計算値に関するデータは、前記媒体識別子に関連するデータを用いて、前記一方向関数計算値を暗号化したデータであることを特徴とする請求項１～４のいずれか１項に記載の電子通帳記録方法。

【請求項６】　前記電子通帳記録方法は、

前記管理コンピュータが、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、記録する段階をさらに有することを特徴とする請求項４又は５に記載の電子通帳記録方法。

【請求項７】　金融機関における取引明細データを記録媒体に記録するための電子通帳登録システムであって、

前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を記録する電子通帳データ記憶手段と、

前記金融機関の金融機関秘密鍵に関するデータを記録した暗号鍵データ記憶手段と、

前記媒体識別子に基づいて前記金融機関秘密鍵で暗号化した金融機関署名データを生成し、前記記録媒体に記録するために前記金融機関署名データを出力する管理コンピュータとを有することを特徴とする電子通帳登録システム。

【請求項８】　前記電子通帳登録システムは、

金融機関口座識別子を記録する金融機関口座データ記憶手段をさらに有し、

前記管理コンピュータは、

前記媒体識別子と前記金融機関口座識別子とに基づいて通帳識別子を生成し、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを特徴とする請求項７に記載の電子通帳登録システム。

【請求項９】　前記管理コンピュータは、

前記記録媒体に記録する取引明細データを抽出し、

前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合し、

認証ができた場合には、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力することを特徴とする請求項７又は８に記載の電子通帳登録システム。

【請求項１０】　前記管理コンピュータは、

一方向関数を用いて、前記取引明細データの一方向関数計算値を算出し、

前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力することを特徴とする請求項７～９のいずれか１項に記載の電子通帳登録システム。

【請求項１１】　前記一方向関数計算値に関するデータは、前記一方向関数計算値を、前記媒体識別子に関連するデータを用いて暗号化したデータであることを特徴とする請求項７～１０のいずれか１項に記載の電子通帳登録システム。

【請求項１２】　前記管理コンピュータは、
既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、前記電子通帳データ記憶手段に、前記生成した一方向関数計算値をさらに記録することを特徴とする請求項１０又は１１に記載の電子通帳登録システム。
【請求項１３】　金融機関における取引明細データを記録するための電子通帳記録媒体であって、
前記電子通帳記録媒体が、前記電子通帳記録媒体の媒体識別子を記録したデータ書込み不可領域と、データ書込み可能領域とを有し、
前記データ書込み可能領域には、前記媒体識別子に関するデータを金融機関秘密鍵で暗号化した金融機関署名データを記録したことを特徴とするコンピュータ読み取り可能な電子通帳記録媒体。
【請求項１４】　前記データ書込み可能領域には、
前記媒体識別子と金融機関口座識別子とに基づいて生成された通帳識別子をさらに記録したことを特徴とする請求項１３に記載のコンピュータ読み取り可能な電子通帳記録媒体。
【請求項１５】　前記データ書込み可能領域には、
前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化したデータをさらに記録したことを特徴とする請求項１３又は１４に記載のコンピュータ読み取り可能な電子通帳記録媒体。
【請求項１６】　前記データ書込み可能領域には、
一方向関数を用いて算出した前記取引明細データの一方向関数計算値に関するデータをさらに記録したことを特徴とする請求項１３～１５のいずれか１項に記載のコンピュータ読み取り可能な電子通帳記録媒体。
【請求項１７】　前記一方向関数計算値に関するデータは、前記一方向関数計算値を前記媒体識別子に関連するデータを用いて暗号化したデータであることを特徴とする請求項１３～１６のいずれか１項に記載のコンピュータ読み取り可能な電子通帳記録媒体。
【請求項１８】　前記データ書込み可能領域には、
既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから生成された一方向関数計算値がさらに記録されていることを特徴とする請求項１６又は１７に記載のコンピュータ読み取り可能な電子通帳記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、銀行口座の利用履歴に関する取引明細データの記録に用いる電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体に関するものである。
【０００２】
【従来の技術】今日、資金を受け取る場合には、金融機関の提供するバンキングサービスを利用して、利用者自身の金融機関口座（例えば、銀行口座）に資金を振り込んでもらうことがある。また、利用者自身も、自身の金融機関口座の資金を他人の金融機関口座に振り込んだりする。一方、現金が必要な場合、利用者自身の金融機関口座から現金を引き出したりする場合もある。このような場合、キャッシュカードを利用して、現金自動預け払い機（ＡＴＭ：Automatic Teller Machine）または現金支払機（ＣＤ：Cash Dispenser）を用いる場合がある。一方、金融機関口座の通帳（例えば、預金通帳）を使用せずに行われた取引明細に関するデータ（未記帳取引明細データ）は、金融機関のシステムに保存されており、金融機関が付与した預金通帳が利用された際にまとめて処理される。具体的には、金融機関口座における取引の内容（取引明細）は、通帳記帳の可能な端末において、その預金通帳に印刷される。このような場合、この預金通帳は、利用者の金融機関に対する預金債権の存在を確認する性格を有するものである。
【０００３】
【発明が解決しようとする課題】しかし、利用者が預金通帳に取引明細を記帳するためには、ＡＴＭや通帳記帳端末等の設置された金融機関の店舗に出向く必要がある。このため、利用者は、迅速に取引状況、現在残高を把握することができなかった。一方、利用者のコンピュータ端末等を用い、電話回線やインターネット等のネットワークを介して金融機関の提供するバンキングサービスを利用して、預金残高照会を行うこともできる。しかし、この預金残高照会結果を印刷しても、預金債権の存在を確認するものとはならない。
【０００４】本発明は、上記問題点を解決するためになされたものであり、その目的は、利用者にとって効率的であり、金融機関にとっても確実に取引明細データを記録した電子通帳を提供することができる電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体を提供することにある。
【０００５】
【課題を解決するための手段】上記問題点を解決するために、請求項１に記載の発明は、管理コンピュータを有する電子通帳登録システムを用いて、金融機関における取引明細データを記録媒体に記録する電子通帳記録方法であって、前記管理コンピュータが、前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を受信し、電子通帳データ記憶手段に記録する第１の段階と、前記管理コンピュータが、前記媒体識別子に基づいて金融機関秘密鍵で暗号化した金融機関署名データを生成する第２の段階と、前記管理コンピュータが、前記金融機関署名データを前記記録媒体に記録するために出力する第３の段階とを有することを要旨とする。
【０００６】請求項２に記載の発明は、請求項１に記載

の電子通帳記録方法において、前記電子通帳記録方法は、前記管理コンピュータが、前記媒体識別子と金融機関口座識別子とに基づいて通帳識別子を生成し、前記電子通帳データ記憶手段に記録する段階をさらに有し、前記第２の段階は、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、前記第３の段階は、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを要旨とする。

【０００７】請求項３に記載の発明は、請求項１又は２に記載の電子通帳記録方法において、前記電子通帳記録方法は、前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合する段階と、認証ができた場合には、前記管理コンピュータが前記記録媒体に記録する取引明細データを抽出する段階と、前記管理コンピュータが、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力する段階とをさらに有することを要旨とする。

【０００８】請求項４に記載の発明は、請求項１～３のいずれか１項に記載の電子通帳記録方法において、前記電子通帳記録方法は、前記管理コンピュータが、一方向関数を用いて前記取引明細データの一方向関数計算値を算出する段階と、前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力する段階とをさらに有することを要旨とする。

【０００９】請求項５に記載の発明は、請求項１～４のいずれか１項に記載の電子通帳記録方法において、前記一方向関数計算値に関するデータは、前記媒体識別子に関連するデータを用いて、前記一方向関数計算値を暗号化したデータであることを要旨とする。

【００１０】請求項６に記載の発明は、請求項４又は５に記載の電子通帳記録方法において、前記電子通帳記録方法は、前記管理コンピュータが、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、記録する段階をさらに有することを要旨とする。

【００１１】請求項７に記載の発明は、金融機関における取引明細データを記録媒体に記録するための電子通帳登録システムであって、前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を記録する電子通帳データ記憶手段と、前記金融機関の金融機関秘密鍵に関するデータを記録した暗号鍵データ記憶手段と、前記媒体識別子に基づいて前記金融機関秘密鍵で暗号化した金融機関署名データを生成し、前記記録媒体に記録するために前記金融機関署名データを出力する管理コンピュータとを有することを要旨とする。

【００１２】請求項８に記載の発明は、請求項７に記載の電子通帳登録システムにおいて、前記電子通帳登録システムは、金融機関口座識別子を記録する金融機関口座データ記憶手段をさらに有し、前記管理コンピュータは、前記媒体識別子と前記金融機関口座識別子とに基づいて通帳識別子を生成し、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを要旨とする。

【００１３】請求項９に記載の発明は、請求項７又は８に記載の電子通帳登録システムにおいて、前記管理コンピュータは、前記記録媒体に記録する取引明細データを抽出し、前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合し、認証ができた場合には、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力することを要旨とする。

【００１４】請求項１０に記載の発明は、請求項７～９のいずれか１項に記載の電子通帳登録システムにおいて、前記管理コンピュータは、一方向関数を用いて、前記取引明細データの一方向関数計算値を算出し、前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力することを要旨とする。

【００１５】請求項１１に記載の発明は、請求項７～１０のいずれか１項に記載の電子通帳登録システムにおいて、前記一方向関数計算値に関するデータは、前記一方向関数計算値を、前記媒体識別子に関連するデータを用いて暗号化したデータであることを要旨とする。

【００１６】請求項１２に記載の発明は、請求項１０又は１１に記載の電子通帳登録システムにおいて、前記管理コンピュータは、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、前記電子通帳データ記憶手段に、前記生成した一方向関数計算値をさらに記録することを要旨とする。

【００１７】請求項１３に記載の発明は、金融機関における取引明細データを記録するための電子通帳記録媒体であって、前記電子通帳記録媒体が、前記電子通帳記録媒体の媒体識別子を記録したデータ書込み不可領域と、データ書込み可能領域とを有し、前記データ書込み可能領域には、前記媒体識別子に関するデータを金融機関秘密鍵で暗号化した金融機関署名データを記録したことを要旨とする。

【００１８】請求項１４に記載の発明は、請求項１３に

記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、前記媒体識別子と金融機関口座識別子とに基づいて生成された通帳識別子をさらに記録したことを要旨とする。

【００１９】請求項１５に記載の発明は、請求項１３又は１４に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化したデータをさらに記録したことを要旨とする。

【００２０】請求項１６に記載の発明は、請求項１３～１５のいずれか１項に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、一方向関数を用いて算出した前記取引明細データの一方向関数計算値に関するデータをさらに記録したことを要旨とする。

【００２１】請求項１７に記載の発明は、請求項１３～１６のいずれか１項に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記一方向関数計算値に関するデータは、前記一方向関数計算値を前記媒体識別子に関連するデータを用いて暗号化したデータであることを要旨とする。

【００２２】請求項１８に記載の発明は、請求項１６又は１７に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから生成された一方向関数計算値がさらに記録されていることを要旨とする。

【００２３】（作用）請求項１又は７に記載の発明によれば、管理コンピュータが、媒体識別子に基づいて金融機関秘密鍵で暗号化した金融機関署名データを生成し、この金融機関署名データを記録媒体に記録するために出力する。このため、この記録媒体を金融機関の提供する電子通帳として利用できる。

【００２４】請求項２又は８に記載の発明によれば、管理コンピュータが、媒体識別子と金融機関口座識別子とに基づいて生成した通帳識別子を金融機関秘密鍵で暗号化して金融機関署名データを生成する。このため、金融機関署名データには、金融機関口座識別子に関するデータが含まれる。従って、一つの記録媒体の中に、複数の金融機関口座に関する通帳を生成できる。

【００２５】請求項３又は９に記載の発明によれば、管理コンピュータが、記録媒体から媒体識別子、通帳識別子の少なくとも一方に関するデータを受信し、受信したデータと電子通帳データ記憶手段に記録されたデータと照合し、認証できれば取引明細に関するデータを送信する。このため、金融機関によって認証されていない記録媒体への取引明細に関するデータの記録を防止できる。また、管理コンピュータは、取引明細データを媒体識別子に関連するデータを用いて暗号化し、記録媒体に記録するために出力する。このため、取引明細データを記録媒体と関連づけて記録できる。従って、取引明細データを、予め定められた記録媒体に安全、確実に記録できる。

【００２６】請求項４又は１０に記載の発明によれば、管理コンピュータが、一方向関数を用いて取引明細データの一方向関数計算値を算出し、記録媒体に記録するために、この一方向関数計算値に関するデータを出力する。このため、記録媒体に記録された取引明細データと一方向関数計算値とから、取引明細データの真正性を担保することができる。

【００２７】請求項５又は１１に記載の発明によれば、一方向関数計算値に関するデータは、前記媒体識別子に関連するデータを用いて、前記一方向関数計算値を暗号化したデータである。このため、取引明細データは媒体識別子と関連づけられ、電子通帳の唯一性を担保できる。

【００２８】請求項６又は１２に記載の発明によれば、管理コンピュータが、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、記録する。このため、一方向関数計算値には、過去の取引明細データが含まれる。これにより、取引明細の連続性を担保でき、一部の取引明細データを削除、追加、改変した場合にも、偽造、改変を確実に把握できる。

【００２９】請求項１３に記載の発明によれば、電子通帳記録媒体には、記録媒体の媒体識別子を記録したデータ書込み不可領域と、媒体識別子に関するデータを金融機関秘密鍵で暗号化した金融機関署名データを記録したデータ書込み可能領域が設けられている。金融機関署名データは、データ書込み不可領域に記録された媒体識別子を用いて生成されるので、偽造、改変を防止できる。そして、金融機関署名データに基づいて、金融機関が提供する通帳であることを認証できる。

【００３０】請求項１４に記載の発明によれば、データ書込み可能領域には、媒体識別子と金融機関口座識別子とに基づいて生成された通帳識別子が、さらに記録されている。このため、金融機関署名データには金融機関口座識別子の情報が含まれ、一つの記録媒体に複数の金融機関口座に関する通帳を生成できる。

【００３１】請求項１５に記載の発明によれば、前記データ書込み可能領域に、取引明細データと、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化したデータがさらに記録されている。このため、取引明細データと媒体識別子とが関連づけられており、他の記録媒体への取引明細データの記録を防止できる。

【００３２】請求項１６に記載の発明によれば、前記データ書込み可能領域に、一方向関数を用いて算出した前

記取引明細データがさらに記録されている。このため、取引明細データとその一方向関数計算値とを照合することでき、取引明細データの真正性を担保することができる。

【００３３】請求項１７に記載の発明によれば、前記一方向関数計算値に関するデータは、前記一方向関数計算値を前記媒体識別子に関連するデータを用いて暗号化したデータである。このため、取引明細データは媒体識別子と関連づけられ、電子通帳の唯一性を担保できる。

【００３４】請求項１８に記載の発明によれば、前記データ書込み可能領域には、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから生成された一方向関数計算値がさらに記録されている。このため、一方向関数計算値には、過去の取引明細データが含まれる。これにより、取引明細の連続性を担保でき、一部の取引明細データを削除、追加、改変した場合にも、偽造、改変を確実に把握できる。

【００３５】

【発明の実施の形態】以下、本発明を具体化した一実施形態を図１～図１０に従って説明する。本実施形態では、利用者が媒体識別子の付与された記録媒体を取得し、この記録媒体を金融機関（ここでは銀行）の取引明細データを記録する場合に用いる電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体として説明する。この電子通帳記録媒体には、通常の預金通帳と同様に取引明細に関する情報が記録され、預金通帳としての機能を有する。

【００３６】図１に示すように、取引明細に関する情報を記録する記録媒体として電子通帳記録媒体１１を用いる。この電子通帳記録媒体１１には、市販の記録媒体を用い、電子通帳記録媒体１１に関する情報を銀行に登録し、所定のデータが記録されることにより電子通帳として機能する。

【００３７】この電子通帳記録媒体１１に未記帳の取引明細データを記録したり、記録された取引明細データを表示したりする場合には、利用者のクライアント端末１０を用いる。クライアント端末１０には、図示しないＣＰＵ、ＲＡＭ、ＲＯＭ等を有するコンピュータであり、各種プログラムの実行、後述するデータの管理、送受信等の制御を行う。さらに、クライアント端末１０には、カードリーダーライター１００が接続されている。このカードリーダーライター１００に電子通帳記録媒体１１を挿入し、電子通帳記録媒体１１に記録されたデータをクライアント端末１０に読み込んだり、電子通帳記録媒体１１にデータを記録したりする。また、このクライアント端末１０には、図示しないディスプレイ装置が接続されている。このディスプレイ装置を用いて、電子通帳記録媒体１１に記録された取引明細を表示する。さらに、クライアント端末１０には、後述するユーザ認証等において、所定のデータを入力するためのデータ入力部が設けられている。

【００３８】このクライアント端末１０は、インターネットＩを介して、電子通帳登録システム２０に接続されている。この電子通帳登録システム２０は、銀行が管理するシステムであり、電子通帳記録媒体１１に関する情報、取引明細に関する情報を管理するコンピュータシステムである。また、電子通帳登録システム２０は、クライアント端末１０にデータを送信したり、クライアント端末１０からのデータを受信したりする。

【００３９】電子通帳登録システム２０は、図１に示すように、管理コンピュータ２１を備えている。この管理コンピュータ２１は、クライアント端末１０の間でデータの送受信を行う。管理コンピュータ２１には、図示しないＣＰＵ、ＲＡＭ、ＲＯＭ等を有するコンピュータであり、各種プログラムの実行、後述するデータの管理、送受信等の制御を行う。

【００４０】管理コンピュータ２１には、未記帳取引明細データ記憶部２２、電子通帳データ記憶手段としての電子通帳データ記憶部２３、金融機関口座データ記憶手段としての銀行口座データ記憶部２４、及び暗号鍵データ記憶手段としての暗号鍵データ記憶部２５が、それぞれ接続されている。

【００４１】以下、図２～６を用いて、電子通帳記録媒体１１及び各記憶部（２２～２５）に記録されるデータを説明する。電子通帳記録媒体１１には、図２に示すように、銀行が電子通帳記録媒体１１を通帳として認証するために必要なデータが記録される。この電子通帳記録媒体１１には、データ書込み不可領域１２０とデータ書込み可能領域１３０とが予め設定されている。このデータ書込み不可領域１２０には、記録媒体を識別するための媒体固有の媒体識別子１２１が予め記録されている。利用者は、このデータ書込み不可領域１２０に記録された媒体識別子１２１を変更することができない。本実施形態では、このような電子通帳記録媒体１１として、データ書込み不可領域１２０を有する著作権保護機能に対応したメモリーカード等を用いる。

【００４２】一方、データ書込み可能領域１３０には、電子通帳データ１３１が記録されている。この電子通帳データ１３１は、暗号鍵データ１３２、通帳識別子データ１３３、暗号化データ１３４、及び多重ハッシュ値データ１３５が記録されている。この暗号鍵データ１３２には、公開鍵暗号方式で用いる媒体秘密鍵１３６と媒体公開鍵１３７とが記録されている。この公開鍵暗号方式は、暗号化する鍵と復号化する鍵とが異なる暗号方式であって、一方を公開し、他方を秘密とする。例えば、公知のＲＳＡ（Rivest-Shamir-Adleman）方式がある。暗号鍵データ１３２は、電子通帳として用いる電子通帳記録媒体１１を定めたときに予め記録される。

【００４３】通帳識別子データ１３３には、通帳識別子

データと銀行署名データとが関連づけられて記録されている。この通帳識別子データ１３３は、利用者がこの記録媒体を電子通帳として銀行に登録の申請を行い、その申請が認められた場合に記録される。本実施形態では、この通帳識別子データ１３３は、通帳識別子毎に銀行署名データが記録されている。通帳識別子データ領域には、電子通帳登録システム２０から付与された通帳識別子に関するデータが記録される。銀行署名データ領域には、電子通帳登録システム２０で生成された銀行署名に関するデータが記録される。

【００４４】暗号化データ１３４には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが、通帳識別子に関連づけられて記録されている。この暗号化データ１３４は、電子通帳登録システム２０から未記帳の取引明細に関してのデータを受信する毎に追加記録される。この暗号化取引明細データ領域には、記帳する取引明細に関するデータを媒体識別子１２１で暗号化したデータが記録される。一方、暗号化ハッシュ値データ領域には、記帳する取引明細に関するデータのハッシュ値を媒体識別子１２１で暗号化したデータが記録される。ここで、ハッシュ値とは、一方向関数としての公知のハッシュ関数を用いてデータを一定の長さ（例えば、１２８ビット）に圧縮した一方向関数計算値である。ハッシュ関数としては、二つの異なるデータのハッシュ値が一致する確率が極めて小さい関数を用いる。

【００４５】多重ハッシュ値データ１３５には、多重ハッシュ値に関するデータが、通帳識別子に関連づけられて記録されている。この多重ハッシュ値データ１３５は、その記帳する取引明細に関してのデータが真正であることが確認された場合に記録される。本実施形態では、この多重ハッシュ値データ１３５は、通帳識別子毎に記録されている。多重ハッシュ値データ領域には、後述するように、既に記録された取引明細に関するデータのハッシュ値と未記帳取引明細に関するデータのハッシュ値とから生成される多重ハッシュ値に関するデータが記録される。

【００４６】未記帳取引明細データ記憶部２２には、図３に示すように、未記帳の取引明細データ２２０が記録されている。この取引明細データ２２０は、利用者が記帳を行った後、新たに取引が行われ、記帳すべき取引明細が発生した場合に記録される。本実施形態では、取引明細データ２２０には、利用者の銀行口座番号と未記帳取引明細とに関するデータが関連付けられて記録されている。この銀行口座番号データ領域には、利用者が保有する銀行口座を特定するための識別子である銀行口座番号が記録される。未記帳取引明細データ領域には、利用者の電子通帳記録媒体１１に記帳されていない取引明細に関するデータが記録される。この未記帳取引明細データ領域に記録されたデータは、電子通帳記録媒体１１に記帳され、クライアント端末１０から後述する記録完了通知を受信した場合に消去される。

【００４７】電子通帳データ記憶部２３には、図４に示すように、利用者が使用する電子通帳に関する電子通帳データ２３０が記録される。この電子通帳データ２３０は、利用者から電子通帳の登録申請があった場合に生成される。本実施形態では、電子通帳データ２３０には、媒体識別子、通帳識別子、媒体公開鍵、最新記帳ハッシュ値、多重ハッシュ値に関するデータが、銀行口座番号に関連づけられて記録される。この媒体識別子データ領域には、利用者が電子通帳として用いる記録媒体の識別子であり、電子通帳記録媒体１１のデータ書込み不可領域１２０に記録された媒体識別子１２１に関するデータが記録される。通帳識別子データ領域には、媒体識別子１２１と銀行口座の属性情報（識別子）に基づいて生成された通帳識別子に関するデータが記録される。媒体公開鍵データ領域には、電子通帳記録媒体１１に記録された媒体公開鍵１３７に関するデータが記録される。この媒体公開鍵は、利用者が電子通帳の登録申請を行った場合に記録される。最新記帳ハッシュ値データ領域には、最後に電子通帳記録媒体１１に記帳された取引明細に関するデータのハッシュ値に関するデータが記録される。多重ハッシュ値データ領域には、過去の多重ハッシュ値と最後に記帳された取引明細データのハッシュ値とから生成された多重ハッシュ値に関するデータが記録される。

【００４８】銀行口座データ記憶部２４には、図５に示すように、利用者の銀行口座に関する銀行口座データ２４０が記録される。この銀行口座データ２４０は、利用者が銀行口座を開設した場合に記録される。本実施形態では、銀行口座データ２４０には、金融機関口座識別子としての銀行口座番号、利用者名、暗証番号に関するデータが、利用者番号に関するデータと関連づけられて記録される。この利用者番号は、銀行が利用者を特定するために付与した識別子である。銀行口座番号データ領域には、銀行口座を特定するためのデータとして、銀行コード、支店コード、口座番号に関するデータが記録される。暗証番号データ領域には、インターネットＩを介して電子通帳登録システム２０にアクセスする場合に用いる本人認証のためのパスワードに関するデータが記録される。

【００４９】暗号鍵データ記憶部２５には、図６に示すように、クライアント端末１０と電子通帳登録システム２０との間で通信を行う場合に用いる銀行の暗号鍵に関する暗号鍵データ２５０が記録される。この暗号鍵データ２５０は、電子通帳登録システム２０を用いて、電子通帳の登録サービスを提供するために予め設定される。本実施形態では、暗号鍵データ２５０には、銀行秘密鍵２５１、銀行公開鍵２５２に関するデータが記録される。これらの鍵は、暗号化を行うための鍵と復号化を行うために用いる鍵である。

【００５０】次に、上記のように構成されたシステムにおいて、電子通帳を利用する場合の処理手順を図７～１０に従って説明する。この場合、大きくは３つの段階からなる。すなわち、図７に示す電子通帳記録媒体１１を登録する段階、図８～９に示す電子通帳登録システム２０から取引明細に関するデータを記録する段階、及び図１０に示す取引明細を表示する段階である。これらの段階では、利用者がクライアント端末１０を用いて処理する。

【００５１】まず、利用者が、クライアント端末１０を用いて電子通帳記録媒体１１を登録する段階の処理を、図７を用いて説明する。まず、利用者はクライアント端末１０を用いてユーザ認証を行う（Ｓ１－１）。この処理は、通常のネットワークを利用したバンキング処理において行われるユーザ認証（本人認証）と同様に行われる。ここでは、まず、利用者はクライアント端末１０を用いてインターネットＩを介して電子通帳登録システム２０にアクセスする。次に、利用者は、電子通帳登録システム２０からの要求に応じて利用者番号、銀行口座番号、暗証番号に関するデータを送信する。データを受信した管理コンピュータ２１は、受信した利用者番号、銀行口座番号、暗証番号が、銀行口座データ記憶部２４に記録された銀行口座データ２４０と一致するかどうかを確認する。両者が一致する場合、管理コンピュータ２１は、ユーザ認証を終了する。そして、管理コンピュータ２１は、電子通帳記録媒体１１の銀行が提供するサービスの利用許諾を利用者に与える。

【００５２】次に、利用者は、クライアント端末１０を用いて電子通帳登録要求を行う（Ｓ１－２）。この場合、クライアント端末１０はインターネットＩを介して、電子通帳登録要求を電子通帳登録システム２０に送信する。電子通帳登録要求を受信した管理コンピュータ２１は、クライアント端末１０に対して媒体識別子要求と銀行公開鍵２５２とを送信する（Ｓ１－３）。この場合、管理コンピュータ２１は、暗号鍵データ記憶部２５から銀行公開鍵２５２を抽出し、クライアント端末１０に送信する。

【００５３】媒体識別子要求を受信したクライアント端末１０は、利用者に対して電子通帳記録媒体１１をカードリーダーライター１００に挿入するように促す。具体的には、クライアント端末１０のディスプレイ装置に、「電子通帳記録媒体の挿入指示」が表示される。さらに、クライアント端末１０は受信した銀行公開鍵２５２を、図示しない記憶部に記録する。次に、電子通帳記録媒体１１がカードリーダーライター１００に挿入された場合、クライアント端末１０は、電子通帳記録媒体１１の媒体識別子１２１を抽出する（Ｓ１－４）。この場合、クライアント端末１０は、カードリーダーライター１００に挿入された電子通帳記録媒体１１のデータ書込み不可領域１２０に記録された媒体識別子１２１を読み出す。次に、クライアント端末１０は、読み出した媒体識別子１２１を暗号化する（Ｓ１－５）。この場合の暗号化には、銀行公開鍵２５２を用いる。

【００５４】次に、クライアント端末１０は、インターネットＩを介して電子通帳登録システム２０に暗号化した媒体識別子１２１と媒体公開鍵１３７に関するデータを送信する（Ｓ１－６）。このデータを受信した管理コンピュータ２１は、暗号化された媒体識別子１２１を銀行秘密鍵２５１で復号化し、媒体識別子を抽出する（Ｓ１－７）。そして、復号化した媒体識別子１２１及び媒体公開鍵１３７を銀行口座番号と関連付けて電子通帳データ記憶部２３に記録する。

【００５５】次に、管理コンピュータ２１は通帳識別子を生成する（Ｓ１－８）。この場合、まず、管理コンピュータ２１は銀行口座データ記憶部２４から、この利用者番号に関連づけられた銀行口座に関するデータを抽出する。ここでは、銀行口座に関するデータとして、支店コードと銀行口座番号を用いる。次に、抽出した銀行口座に関するデータと媒体識別子とから通帳識別子を生成する。そして、管理コンピュータ２１は生成した通帳識別子を電子通帳データ記憶部２３に記録する。次に、管理コンピュータ２１は、生成した通帳識別子を媒体公開鍵１３７で暗号化し、暗号化通帳識別子を生成する（Ｓ１－９）。さらに、管理コンピュータ２１は、電子通帳データ記憶部２３に記録した通帳識別子を、銀行秘密鍵２５１で暗号化して銀行電子署名データを生成する（Ｓ１－１０）。

【００５６】次に、管理コンピュータ２１は、インターネットＩを介して、暗号化通帳識別子及び銀行電子署名に関するデータをクライアント端末１０に送信する（Ｓ１－１１）。このデータを受信したクライアント端末１０は、受信した暗号化通帳識別子を媒体秘密鍵１３６で復号化して通帳識別子を抽出する（Ｓ１－１２）。そして、クライアント端末１０は通帳識別子、銀行電子署名を電子通帳記録媒体１１に記録する（Ｓ１－１３）。記録が完了した場合には、クライアント端末１０は、電子通帳登録システム２０にインターネットＩを介して記録完了通知を送信する（Ｓ１－１４）。以上により、電子通帳記録媒体１１の登録処理を終了する。

【００５７】次に、利用者がクライアント端末１０を用いて電子通帳記録媒体１１に未記帳の取引明細に関するデータを記録する段階の処理を、図８～９を用いて説明する。まず、利用者は、クライアント端末１０を用いてユーザ認証を行う（Ｓ２－１）。この処理は、上述したステップ（Ｓ１－１）と同様に、ユーザ認証（本人認証）と同様に行われる。具体的には、まず、利用者はクライアント端末１０を用いてインターネットＩを介して電子通帳登録システム２０にアクセスする。次に、利用者は、電子通帳登録システム２０からの要求に応じて利用者番号、銀行口座番号、暗証番号に関するデータを送

信する。データを受信した管理コンピュータ２１は、受信した利用者番号、銀行口座番号、暗証番号が、銀行口座データ記憶部２４に記録された銀行口座データ２４０と一致するかどうかを確認する。管理コンピュータ２１は、一致する場合には、ユーザ認証を終了し、銀行が提供するサービスの許諾を利用者に与える。

【００５８】次に、利用者は、クライアント端末１０を用いて電子通帳記帳要求を行う（Ｓ２－２）。この場合、クライアント端末１０は、インターネットＩを介して電子通帳記帳要求を、電子通帳登録システム２０に送信する。

【００５９】電子通帳記帳要求を受信した管理コンピュータ２１は、クライアント端末１０に対して通帳識別子要求と銀行公開鍵２５２とを送信する（Ｓ２－３）。この場合、管理コンピュータ２１は、暗号鍵データ記憶部２５から銀行公開鍵２５２を抽出して送信する。

【００６０】通帳識別子要求を受信したクライアント端末１０は、利用者に対して電子通帳記録媒体１１をカードリーダーライター１００に挿入するように促す。具体的には、クライアント端末１０のディスプレイ装置に、「電子通帳記録媒体の挿入指示」が表示される。さらに、クライアント端末１０は受信した銀行公開鍵２５２を図示しない記憶部に記録する。次に、クライアント端末１０は、電子通帳記録媒体１１に記録された通帳識別子を抽出する（Ｓ２－４）。この場合、クライアント端末１０はカードリーダーライター１００に挿入された電子通帳記録媒体１１のデータ書込み可能領域１３０に記録された通帳識別子、多重ハッシュ値に関するデータを読み出す。

【００６１】電子通帳記録媒体１１に複数の口座識別子が記録されている場合には、それらのクライアント端末１０のディスプレイ装置に表示し、利用者に電子通帳の選択を促す。そして、クライアント端末１０は選択された通帳識別子の多重ハッシュ値を読み出す。なお、初めて電子通帳記録媒体１１を用いて記帳する場合には、電子通帳記録媒体１１には多重ハッシュ値は記録されていないので、通帳識別子のみを読み出す。次に、クライアント端末１０は、読み出した通帳識別子及び多重ハッシュ値（初めて記帳する場合には通帳識別子）を暗号化して暗号化データを生成する（Ｓ２－５）。この場合の暗号化には、銀行公開鍵２５２を用いる。

【００６２】次に、クライアント端末１０は、インターネットＩを介して電子通帳登録システム２０に暗号化データを送信する（Ｓ２－６）。この暗号化データを受信した管理コンピュータ２１は、暗号化データを復号化し、通帳識別子、多重ハッシュ値を抽出する（Ｓ２－７）。この場合、管理コンピュータ２１は暗号鍵データ記憶部２５に記録された銀行秘密鍵２５１を用いて復号化する。なお、この場合も、初めて記帳する場合には、管理コンピュータ２１は通帳識別子のみを抽出する。次に、管理コンピュータ２１は復号化した通帳識別子、多重ハッシュ値の照合を行う（Ｓ２－８）。この場合、管理コンピュータ２１は、この処理における銀行口座番号に関連づけられて記録された電子通帳データ２３０の通帳識別子、多重ハッシュ値と、復号化した通帳識別子、多重ハッシュ値とが一致するかどうかを照合する。なお、電子通帳データ２３０に多重ハッシュ値の記録がない場合（初めて記帳する場合）には、管理コンピュータ２１は通帳識別子のみを照合する。

【００６３】通帳識別子、多重ハッシュ値が一致しない場合（ステップ（Ｓ２－８）において「Ｎｏ」の場合）、管理コンピュータ２１はインターネットＩを介してクライアント端末１０に取引明細データの記帳拒否を送信する（Ｓ２－９）。記帳拒否を受信したクライアント端末１０のディスプレイ装置には、その旨が表示される。通帳識別子、多重ハッシュ値が一致し、認証ができた場合（「Ｙｅｓ」の場合）、管理コンピュータ２１は未記帳明細データのハッシュ値（未記帳明細ハッシュ値）を生成する（Ｓ２－１０）。ここでは、管理コンピュータ２１は未記帳取引明細データ記憶部２２から銀行口座番号に関連づけられた取引明細データ２２０を抽出し、ハッシュ関数を用いて未記帳明細ハッシュ値を算出する。そして、管理コンピュータ２１は、生成したハッシュ値を電子通帳データ２３０の最新記帳ハッシュ値データ領域に記録する。この場合、既に最新記帳ハッシュ値データ領域にデータが記録されている場合は、算出した未記帳ハッシュ値に置き換える。

【００６４】次に、管理コンピュータ２１は、多重ハッシュ値を生成する（Ｓ２－１１）。具体的には、まず、電子通帳データ記憶部２３に記録されている多重ハッシュ値を抽出する。そして、管理コンピュータ２１は、この多重ハッシュ値と未記帳明細ハッシュ値とから多重ハッシュ値を生成する。この場合、抽出した多重ハッシュ値と未記帳明細ハッシュ値とを結合し、そのデータをハッシュ関数に導入してハッシュ値を算出する。

【００６５】次に、管理コンピュータ２１は、算出した多重ハッシュ値を、電子通帳データ２３０の多重ハッシュ値データ領域に記録する（Ｓ２－１２）。この場合、既に多重ハッシュ値データ領域にデータが記録されている場合は、算出した多重ハッシュ値に置き換える。

【００６６】次に、管理コンピュータ２１は、未記帳明細データ、未記帳明細ハッシュ値を媒体識別子で暗号化する（Ｓ２－１３）。この場合、まず、管理コンピュータ２１は電子通帳データ記憶部２３に記録された媒体識別子を抽出する。次に、管理コンピュータ２１は、抽出した媒体識別子を用いて、未記帳明細データ、未記帳明細ハッシュ値を個別に暗号化することにより、暗号化取引明細データ、暗号化ハッシュ値を生成する。

【００６７】次に、管理コンピュータ２１は、インターネットＩを介して暗号化したデータをクライアント端末

１０に送信する（Ｓ２－１４）。クライアント端末１０は、電子通帳記録媒体１１に受信したデータを記録する（Ｓ２－１５）。この場合、クライアント端末１０は、受信したデータを通帳識別子に関連づけて暗号化データ１３４として電子通帳記録媒体１１に追加記録する。

【００６８】次に、クライアント端末１０は受信したデータの復号化を行う（Ｓ２－１６）。ここでは、まず、クライアント端末１０は電子通帳記録媒体１１に記録された媒体識別子１２１を抽出する。次に、クライアント端末１０は、媒体識別子１２１を用い、受信した暗号化取引明細データ、暗号化ハッシュ値を復号化し、未記帳明細データ、未記帳明細ハッシュ値を抽出する。

【００６９】次に、クライアント端末１０は、抽出した未記帳明細データと未記帳明細ハッシュ値とを照合する（Ｓ２－１７）。具体的には、クライアント端末１０は、ハッシュ関数を用いて未記帳明細データのハッシュ値を算出し、抽出した未記帳明細ハッシュ値と算出したハッシュ値とが一致するかどうかを確認する。抽出した未記帳明細ハッシュ値と算出したハッシュ値とが一致しない場合、クライアント端末１０はエラーを出力し、処理を終了する。

【００７０】抽出した未記帳明細ハッシュ値と算出したハッシュ値とが一致する場合、クライアント端末１０は、多重ハッシュ値を生成する（Ｓ２－１８）。具体的には、まず、クライアント端末１０は電子通帳記録媒体１１に記録されている多重ハッシュ値を抽出する。そして、クライアント端末１０は、この多重ハッシュ値と未記帳明細ハッシュ値とから多重ハッシュ値を生成する。この場合、抽出した多重ハッシュ値と未記帳明細ハッシュ値とを結合し、そのデータをハッシュ関数に導入してハッシュ値を算出する。そして、クライアント端末１０は、算出した多重ハッシュ値を、通帳識別子と関連づけて多重ハッシュ値データ１３５の多重ハッシュ値データ領域に記録する。この場合、既に多重ハッシュ値データ領域にデータが記録されている場合は、算出した多重ハッシュ値に置き換える。そして、クライアント端末１０はインターネットＩを介して電子通帳登録システム２０に記録完了の通知する（Ｓ２－１９）。記録完了通知を受信した管理コンピュータ２１は、この未記帳取引明細データ記憶部２２に記録された取引明細データ２２０を消去する。以上により、電子通帳記録媒体１１への取引明細データの記録処理を終了する。

【００７１】次に、利用者が、クライアント端末１０を用いて取引明細を表示する段階の処理を、図１０を用いて説明する。まず、利用者は、クライアント端末１０を用いて電子通帳の表示要求を入力する（Ｓ３－１）。この場合、クライアント端末１０は利用者に対して、電子通帳記録媒体１１をカードリーダーライター１００に挿入するように促す。次に、クライアント端末１０は、電子通帳記録媒体１１に記録されているすべての通帳識別子を抽出する（Ｓ３－２）。

【００７２】次に、クライアント端末１０は抽出した通帳識別子をディスプレイ装置に表示して、利用者に対して通帳識別子の選択を促す（Ｓ３－３）。通帳識別子が選択された場合には、クライアント端末１０は、データ書込み不可領域１２０に記録された媒体識別子１２１、及び選択された通帳識別子に関連づけられて記録された暗号化データ１３４を抽出する（Ｓ３－４）。次に、クライアント端末１０は抽出した媒体識別子１２１で暗号化データ１３４の暗号化取引明細データ、暗号化ハッシュ値を復号化する（Ｓ３－５）。

【００７３】次に、取引明細データに関してハッシュ値の検証する（Ｓ３－６）。この場合、クライアント端末１０は取引明細データをハッシュ関数に導入し、ハッシュ値を算出し、抽出したハッシュ値と比較する。両者が不一致の場合は、取引明細の表示を拒否する（Ｓ３－７）。両者が一致する場合は、クライアント端末１０は取引明細を表示する（Ｓ３－８）。以上により、取引明細の表示処理を終了する。

【００７４】以上、本実施形態によれば、以下に示す効果を得ることができる。

・　上記実施形態では、電子通帳記録媒体１１として、媒体識別子１２１の記録されたデータ書込み不可領域１２０を有する記録媒体を用いる。このような記録媒体は市販されているので、利用者のハードウエア、通信等の環境や好み等に応じて、取引明細データを記録する媒体を選択して通帳を作成することができる。さらに、媒体識別子１２１はデータ書込み不可領域１２０に記録されているので、電子通帳の複製など偽造を防止できる。

【００７５】・　上記実施形態では、電子通帳記録媒体１１には暗号化された取引明細に関するデータが記録されている。このため、このデータを媒体識別子１２１で復号化すれば、取引明細データをクライアント端末１０に電子的に取り込むことが可能である。従って、この取引明細データを家計簿等に容易に加工できる。

【００７６】・　上記実施形態では、電子通帳記録媒体１１には、通帳識別子データ１３３が記録されている。このため、銀行の預金通帳としての電子通帳記録媒体１１を客観的に認証できる。

【００７７】・　上記実施形態では、電子通帳記録媒体１１には、通帳識別子データ１３３と銀行署名データとが関連づけられて記録されている。この通帳識別子は、媒体識別子１２１に基づいて生成されるため、電子通帳記録媒体１１に記録された取引明細データを複製し、真正な電子通帳記録媒体１１以外への記録を防止できる。さらに、この通帳識別子には、銀行口座識別子に関する情報を含んでいるので、電子通帳記録媒体１１に複数の銀行口座に関する銀行署名データを記録させることができる。

【００７８】・　上記実施形態では、暗号化データ１３

４には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが、通帳識別子に関連づけられて記録されている。このため、複数の銀行口座に対して通帳識別子毎に取引明細データを電子通帳記録媒体１１に記録することができる。従って、従来のように銀行口座毎に通帳を持つ必要がなく、通帳管理の自由度を大きくすることができる。

【００７９】・　上記実施形態では、暗号化データ１３４には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが、通帳識別子に関連づけられて記録されている。この暗号化取引明細データと暗号化ハッシュ値は、媒体識別子１２１を用いて暗号化されている。暗号化取引明細データと暗号化ハッシュ値とを他の電子通帳記録媒体１１に記録した場合、媒体識別子１２１が異なるので、暗号化取引明細データを正確に復号化できない。さらに、取引明細データとそのハッシュ値が不一致になるので、取引明細が表示されない。従って、取引明細データの複製、真正な電子通帳記録媒体１１以外への記録を防止できる。

【００８０】・　上記実施形態では、暗号化データ１３４には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが関連づけられて記録されている。このため、ハッシュ関数を用いることにより、データの真正性を容易に検証することができる。

【００８１】・　上記実施形態では、多重ハッシュ値データ１３５には、多重ハッシュ値に関するデータが、通帳識別子に関連づけられて記録されている。この多重ハッシュ値は、過去の取引明細に関する情報を含むため、一部の取引明細データを削除、追加、改変した場合にも、多重ハッシュ値の相違から、偽造、改変を確実に把握できる。

【００８２】・　上記実施形態では、電子通帳データ記憶部２３には、図４に示すように、利用者が使用する電子通帳に関する電子通帳データ２３０が記録される。そして、電子通帳データ２３０には、媒体識別子、通帳識別子、媒体公開鍵、最新記帳ハッシュ値、多重ハッシュ値に関するデータが、銀行口座番号に関するデータと関連づけられて記録される。このため、銀行が認めた電子通帳記録媒体１１を確実に特定できる。

【００８３】・　上記実施形態では、管理コンピュータ２１は、未記帳明細データ、未記帳明細ハッシュ値を暗号化し、クライアント端末１０に送信する。この暗号化には媒体識別子１２１が用いた共通鍵暗号方式を用いる。このため、守秘性を担保した暗号化が容易にでき、管理コンピュータ２１、クライアント端末１０の暗号化、復号化の負荷を軽減できる。

【００８４】なお、上記実施形態は、以下の態様に変更してもよい。

・　上記実施形態では、通帳識別子を銀行秘密鍵２５１で暗号化して銀行署名データを生成した。これに代えて、媒体識別子１２１のみを銀行秘密鍵２５１で暗号化して銀行署名データを生成してもよい。この場合、電子通帳記録媒体１１に記録する電子通帳は一つの銀行口座とする。これにより、媒体識別子１２１に基づいて生成された銀行署名データであれば、通帳としての電子通帳記録媒体１１を客観的に認証できる。

【００８５】・　上記実施形態では、ステップ（Ｓ２－３）において、管理コンピュータ２１はクライアント端末１０に対して通帳識別子要求と銀行公開鍵２５２とを送信した。これに代えて、媒体識別子１２１を要求してもよい。この場合、電子通帳記録媒体１１に記録する電子通帳は一つの銀行口座とする。これにより、媒体識別子１２１に基づいて電子通帳記録媒体１１を認証できる。

【００８６】・　上記実施形態では、管理コンピュータ２１やクライアント端末１０は、銀行公開鍵や媒体公開鍵を、相手方に送信した。これに代えて、必要に応じて認証登録証明機関のシステムから公開された鍵を取得してもよい。これにより、電子通帳データ記憶部２３に媒体公開鍵を記録する必要がなくなる。

【００８７】・　上記実施形態では、管理コンピュータ２１は、通帳記帳の際には、通帳識別子、多重ハッシュ値を用いて、電子通帳記録媒体１１の真正性を確認した。これに代えて、暗号化データ１３４の暗号化ハッシュ値を用いて真正性を確認してもよい。この場合には、図１１～１２に示す手順を用いる。上記実施形態と同様に、クライアント端末１０と電子通帳登録システム２０との間でユーザ認証を行う（Ｓ４－１）。次に、クライアント端末１０は電子通帳記帳要求を送信し（Ｓ４－２）、管理コンピュータ２１は通帳識別子要求、銀行公開鍵を送信する（Ｓ４－３）。ここで、クライアント端末１０は、通帳識別子、最後に記録された暗号化ハッシュ値を抽出する（Ｓ４－４）。そして、通帳識別子、抽出した暗号化ハッシュ値を銀行公開鍵で暗号化し（Ｓ４－５）、このデータを電子通帳登録システム２０に送信する（Ｓ４－６）。

【００８８】管理コンピュータ２１は、受信したデータを銀行秘密鍵で復号化して通帳識別子、暗号化ハッシュ値を抽出する（Ｓ４－７）。さらに、暗号化ハッシュ値を媒体識別子で復号化してハッシュ値を抽出する（Ｓ４－８）。次に、管理コンピュータ２１は、抽出したハッシュ値と電子通帳データ記憶部２３に記録された最新記帳ハッシュ値との照合を行う（Ｓ４－９）。両者が一致しない場合は、管理コンピュータ２１はクライアント端末１０に記帳拒否を通知する（Ｓ４－１０）。両者が一致する場合は、管理コンピュータ２１は、未記帳明細データのハッシュ値を生成する（Ｓ４－１１）。そして、未記帳明細データ、未記帳明細ハッシュ値を媒体識別子で暗号化し、クライアント端末１０に送信する（Ｓ４－１２）。

【００８９】クライアント端末１０は、受信したデータを電子通帳記録媒体１１に記録する（Ｓ４－１３）。この場合、上記実施形態と同様に、クライアント端末１０は、暗号化未記帳明細データを暗号化取引明細データとして、暗号化未記帳明細ハッシュ値を暗号化ハッシュ値として記録する。さらに、クライアント端末１０は、受信したデータを復号化する（Ｓ４－１４）。そして、未記帳明細データと未記帳明細ハッシュ値とを比較し、照合する（Ｓ４－１５）。次に、クライアント端末１０は、電子通帳記録媒体１１に記録された多重ハッシュ値を抽出する（Ｓ４－１６）。そして、電子通帳記録媒体１１に記録されていた多重ハッシュ値及び未記帳明細ハッシュ値から、新しい多重ハッシュ値を生成し（Ｓ４－１７）、電子通帳記録媒体１１に多重ハッシュ値として上書き記録する（Ｓ４－１８）。その後、クライアント端末１０は、電子通帳登録システム２０に記録完了の通知を行う（Ｓ４－１９）。この場合、電子通帳データ記憶部２３に多重ハッシュ値を記録しておく必要がなく、電子通帳データ記憶部２３に記憶容量を削減できる。

【００９０】・　上記実施形態では、多重ハッシュ値は、過去の多重ハッシュ値と未記帳明細データのハッシュ値とを用いて生成した。これに代えて、最初の多重ハッシュ値は通帳識別子から生成してもよい。これにより、電子通帳記録媒体１１の真正性と取引明細データの真正性とを、より確実に担保できる。

【００９１】・　上記実施形態では、ステップ（Ｓ３－４）において、通帳識別子が選択された場合には、クライアント端末１０は、データ書込み不可領域１２０に記録された媒体識別子１２１及び選択された通帳識別子に関連づけられて記録された暗号化データ１３４を抽出した。これに代えて、表示させる取引明細の範囲を指定させてもよい。この場合、まず、クライアント端末１０は利用者に、表示させる取引明細の範囲の入力を促す。そして、クライアント端末１０は暗号化データ１３４を抽出し、指定された範囲の取引明細データに関するハッシュ値のみを抽出し、ステップ（Ｓ３－５）～（Ｓ３－８）を実行する。これにより、クライアント端末１０の負荷を軽減しながら、利用者が所望の取引明細のみを表示することができる。

【００９２】・　上記実施形態では、ステップ（Ｓ２－１５）において、クライアント端末１０が、受信したデータを通帳識別子に関連づけて暗号化データ１３４として電子通帳記録媒体１１に記録した。これに代えて、クライアント端末１０は受信したデータをそのまま電子通帳記録媒体１１に記録してもよい。この場合は、管理コンピュータ２１が、暗号化したデータに通帳識別子を関連づけて送信する。これにより、クライアント端末１０の処理を削減できる。

【００９３】・　上記実施形態では、ステップ（Ｓ２－１７）において、抽出した未記帳明細ハッシュ値と算出したハッシュ値とが一致しない場合、クライアント端末１０はエラーを出力し、処理を終了した。これに加え、クライアント端末１０が管理コンピュータ２１にエラーのあったことを送信してもよい。この場合、管理コンピュータ２１は元の未記帳ハッシュ値、多重ハッシュ値を仮記憶しておき、クライアント端末１０からエラーを受信した場合には、未記帳ハッシュ値、多重ハッシュ値を元の値に戻す。これにより、エラー時にもデータを維持でき、正確な記帳が可能である。

【００９４】・　上記実施形態では、一つの銀行口座に対して一つの電子通帳記録媒体１１を用いたが、途中で電子通帳記録媒体１１を変更させてもよい。この場合、図７に示す電子通帳記録媒体１１の登録処理を再度行う。その場合、管理コンピュータ２１は、電子通帳データ記憶部２３に記録された媒体識別子、通帳識別子、媒体公開鍵を、新しい電子通帳記録媒体１１にあわせて変更する。これにより、電子通帳記録媒体１１のデータ書込み可能領域１３０が飽和した場合や利用者が新しい電子通帳記録媒体１１に取引明細データを記録する場合にも対応できる。

【００９５】・　上記実施形態では、電子通帳記録媒体１１に記録する取引明細データ、ハッシュ値は媒体識別子１２１で暗号化した。暗号化に用いる鍵は媒体識別子そのものを使用する必要はなく、これに代えて、通帳識別子で暗号化してもよい。通帳識別子は、媒体識別子１２１と銀行口座に関するデータとから生成されるため、銀行口座に関する情報に関連づけた暗号化を実現できる。

【００９６】・　上記実施形態では、クライアント端末１０／電子通帳登録システム２０間をインターネットＩで接続した。この代わりに、専用線や公衆回線を用いて接続してもよい。この場合、仮想的な専用線であってもよい。これにより、より安全に取引を行うことができる。

【００９７】・　上記実施形態では、電子通帳登録システム２０に、各記憶部（２２～２５）を設けたが、他のシステムの記憶部を利用してもよい。例えば、銀行口座データ記憶部２４は、銀行が有する他のシステムに設置してもよい。これにより、既存の銀行口座に関するデータを利用できる。

【００９８】・　上記実施形態では、取引明細を表示する端末としてクライアント端末１０を用いた。これに代えて、電子通帳記録媒体１１に記録されたデータを読み込むことができる携帯電話端末やＰＤＡ（Personal Digital Assistant）を用いてもよい。また、クライアント端末１０として双方向テレビジョン端末を用いてもよい。この場合、電子通帳登録システム２０から利用者に向けて情報を流す下りチャネルと、利用者から電子通帳登録システム２０にデータを送る上りチャネルとを準備する。これにより、色々な端末を用いて、取引明細を表

示させることができる。

【００９９】・　上記実施形態では、電子通帳記録媒体１１として、記録媒体を用いた。これに代えて、データ書込み不可領域１２０が設定された記憶端末を用いてもよい。この場合も、データ書込み不可領域１２０には、その端末を特定する識別子を事前に記録しておく。これにより、記録媒体の自由度を確保することができる。

【０１００】

【発明の効果】以上詳述したように、本発明によれば、金融機関における取引明細データを記録媒体に記録させることができるので、利用者にとって迅速に取引明細を取得できる。また、取引明細データの加工も容易である。一方、金融機関にとっても、真正性を担保した電子通帳を利用者に提供できる。

【図面の簡単な説明】

【図１】　本発明の実施形態のシステム概略図。

【図２】　電子通帳記録媒体に記録されたデータの説明図。

【図３】　未記帳取引明細データ記憶部に記録されたデータの説明図。

【図４】　電子通帳データ記憶部に記録されたデータの説明図。

【図５】　銀行口座データ記憶部に記録されたデータの説明図。

【図６】　暗号鍵データ記憶部に記録されたデータの説明図。

【図７】　本実施形態の処理手順の説明図。

【図８】　本実施形態の処理手順の説明図。

【図９】　本実施形態の処理手順の説明図。

【図１０】　本実施形態の処理手順の説明図。

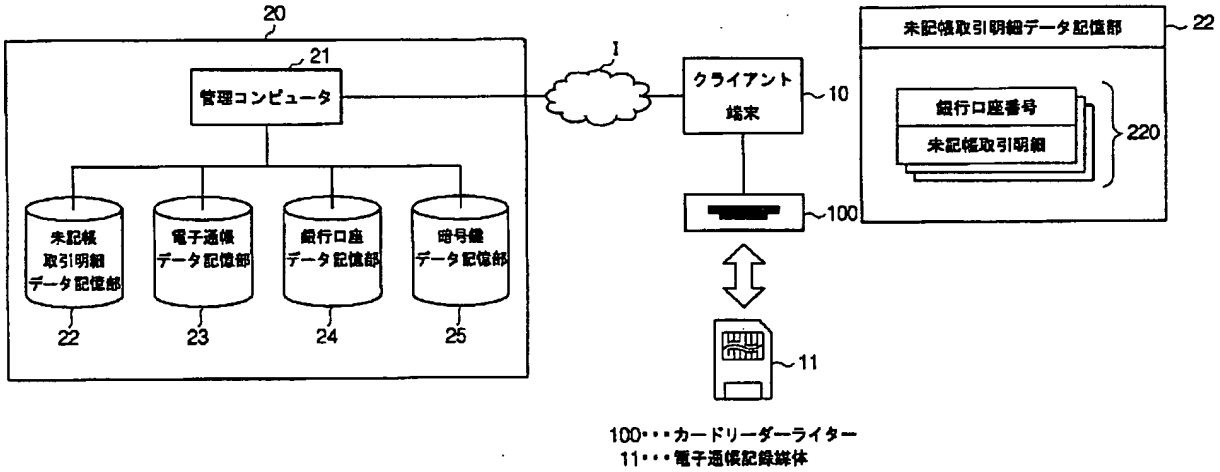
【図１１】　他の実施形態の処理手順の説明図。

【図１２】　他の実施形態の処理手順の説明図。

【符号の説明】

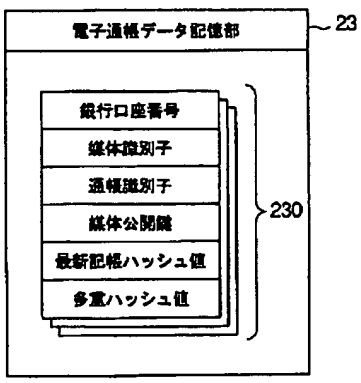
１０…クライアント端末、１１…電子通帳記録媒体、１２０…データ書込み不可領域、２０…電子通帳登録システム、２１…管理コンピュータ、２３…電子通帳データ記憶手段としての電子通帳データ記憶部、２４…銀行口座データ記憶手段としての銀行口座データ記憶部、２５…暗号鍵データ記憶手段としての暗号鍵データ記憶部、Ｉ…インターネット。

【図１】

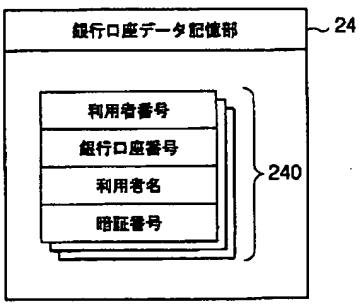


【図３】

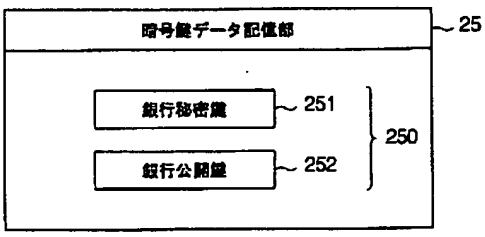
【図４】



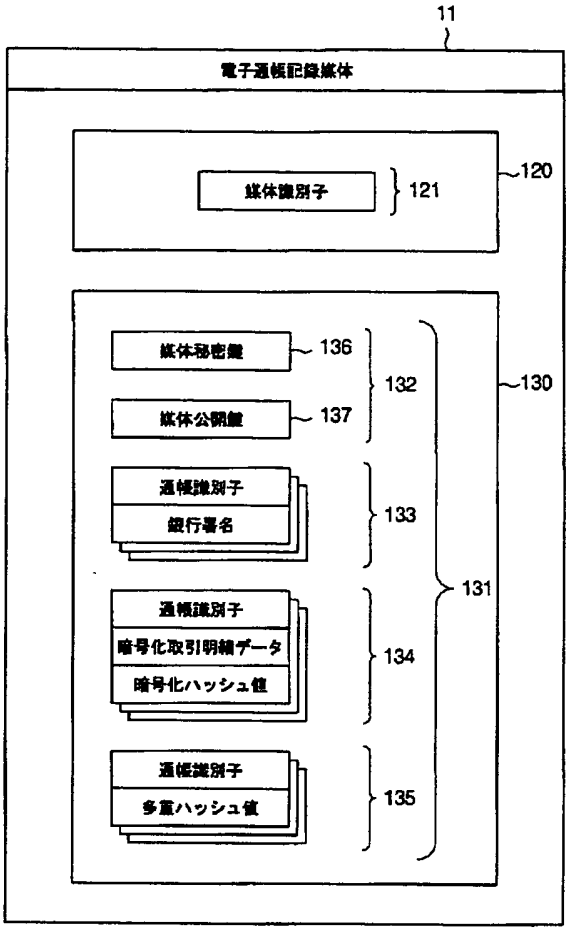
【図５】



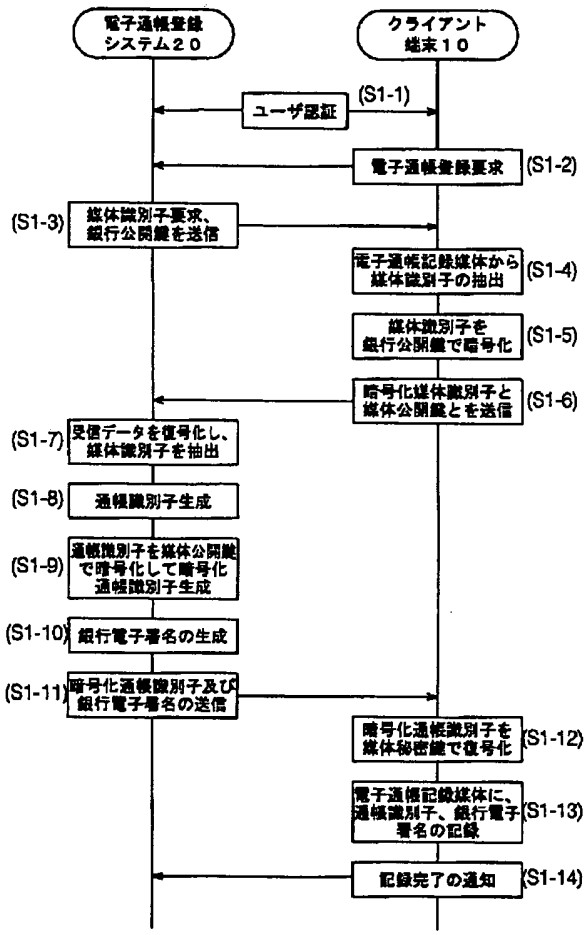
【図６】



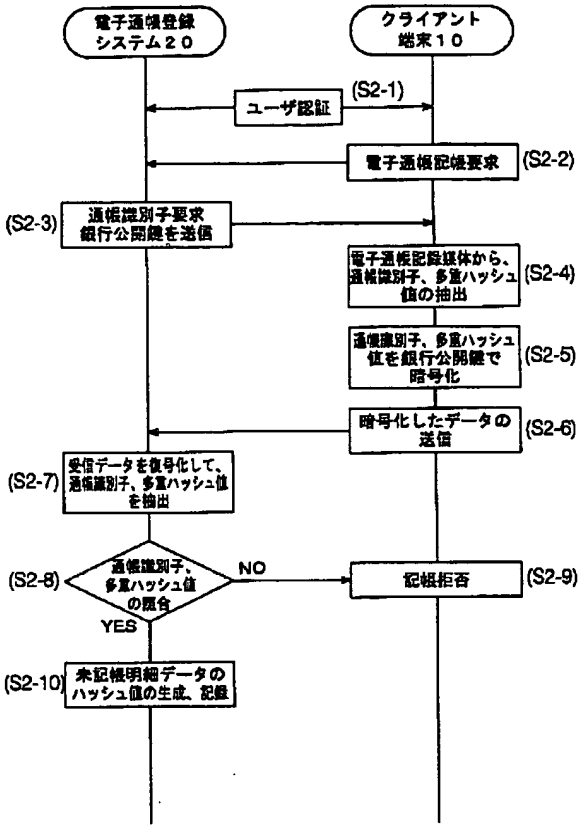
【図２】


11
電子通帳記録媒体
媒体識別子
121
120
媒体秘密鍵
136
媒体公開鍵
137
132
130
通帳識別子
銀行署名
133
通帳識別子
暗号化取引明細データ
暗号化ハッシュ値
134
131
通帳識別子
多重ハッシュ値
135

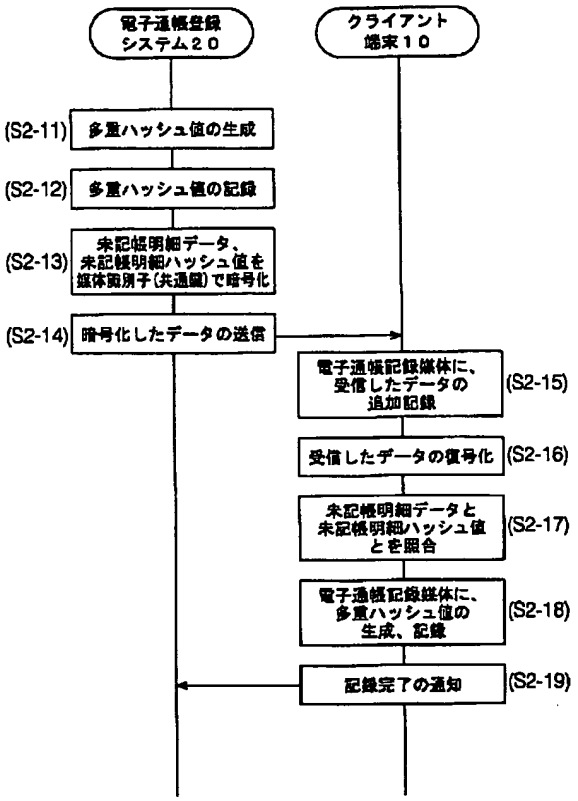
【図７】


電子通帳登録システム２０
クライアント端末１０
ユーザ認証
(S1-1)
電子通帳登録要求
(S1-2)
(S1-3)
媒体識別子要求、銀行公開鍵を送信
電子通帳記録媒体から媒体識別子の抽出
(S1-4)
媒体識別子を銀行公開鍵で暗号化
(S1-5)
暗号化媒体識別子と媒体公開鍵とを送信
(S1-6)
(S1-7)
受信データを復号化し、媒体識別子を抽出
(S1-8)
通帳識別子生成
(S1-9)
通帳識別子を媒体公開鍵で暗号化して暗号化通帳識別子生成
(S1-10)
銀行電子署名の生成
(S1-11)
暗号化通帳識別子及び銀行電子署名の送信
暗号化通帳識別子を媒体秘密鍵で復号化
(S1-12)
電子通帳記録媒体に、通帳識別子、銀行電子署名の記録
(S1-13)
記録完了の通知
(S1-14)

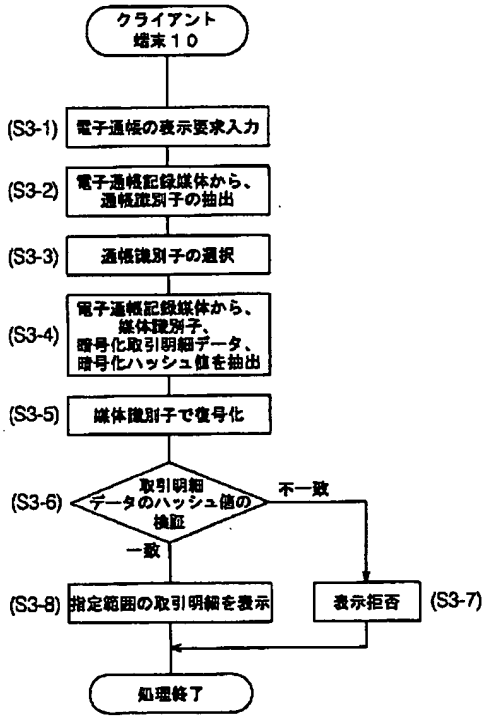
【図８】


電子通帳登録システム２０
クライアント端末１０
ユーザ認証
(S2-1)
電子通帳記帳要求
(S2-2)
(S2-3)
通帳識別子要求
銀行公開鍵を送信
電子通帳記録媒体から、通帳識別子、多重ハッシュ値の抽出
(S2-4)
通帳識別子、多重ハッシュ値を銀行公開鍵で暗号化
(S2-5)
暗号化したデータの送信
(S2-6)
(S2-7)
受信データを復号化して、通帳識別子、多重ハッシュ値を抽出
(S2-8)
通帳識別子、多重ハッシュ値の照合
NO
記帳拒否
(S2-9)
YES
(S2-10)
未記帳明細データのハッシュ値の生成、記録

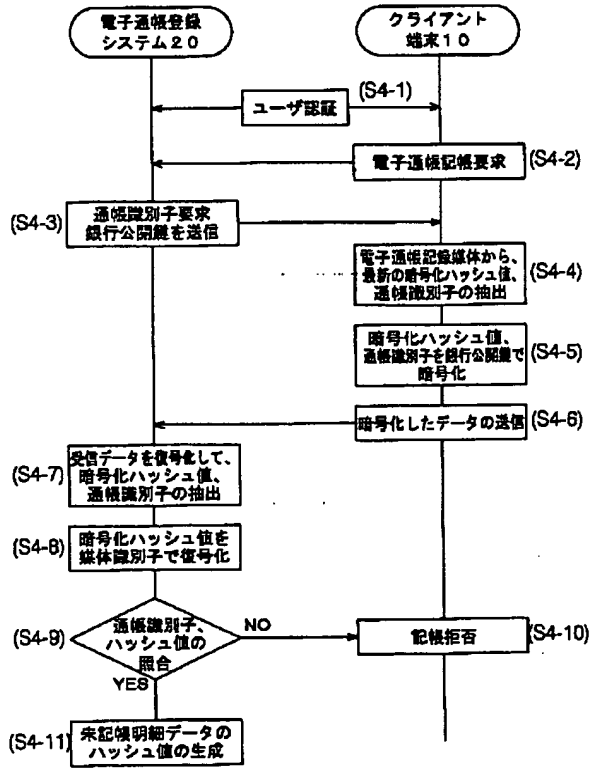
【図９】


電子通帳登録システム２０
クライアント端末１０
(S2-11)
多重ハッシュ値の生成
(S2-12)
多重ハッシュ値の記録
(S2-13)
未記帳明細データ、未記帳明細ハッシュ値を媒体識別子(共通鍵)で暗号化
(S2-14)
暗号化したデータの送信
電子通帳記録媒体に、受信したデータの追加記録
(S2-15)
受信したデータの復号化
(S2-16)
未記帳明細データと未記帳明細ハッシュ値とを照合
(S2-17)
電子通帳記録媒体に、多重ハッシュ値の生成、記録
(S2-18)
記録完了の通知
(S2-19)

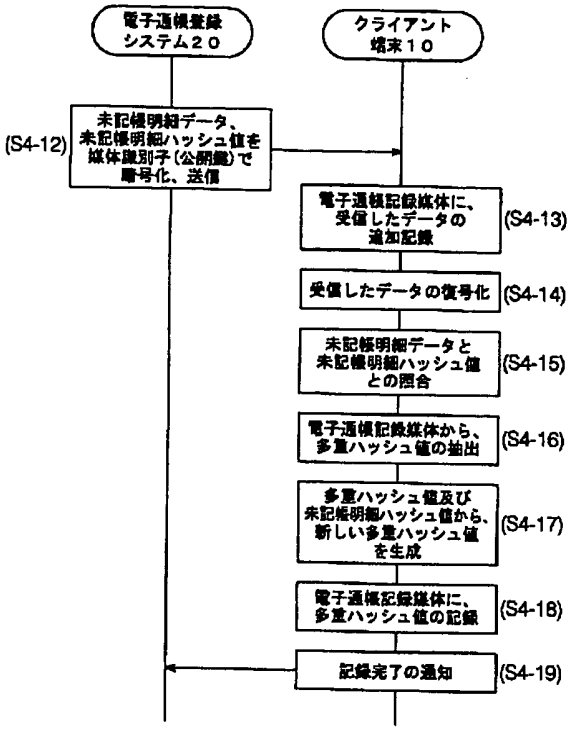
【図１０】


クライアント端末１０
(S3-1)
電子通帳の表示要求入力
(S3-2)
電子通帳記録媒体から、通帳識別子の抽出
(S3-3)
通帳識別子の選択
(S3-4)
電子通帳記録媒体から、媒体識別子、暗号化取引明細データ、暗号化ハッシュ値を抽出
(S3-5)
媒体識別子で復号化
(S3-6)
取引明細データのハッシュ値の検証
不一致
一致
(S3-8)
指定範囲の取引明細を表示
表示拒否
(S3-7)
処理終了

【図１１】


電子通帳登録システム２０
クライアント端末１０
ユーザ認証
(S4-1)
電子通帳記帳要求
(S4-2)
(S4-3)
通帳識別子要求
銀行公開鍵を送信
電子通帳記録媒体から、最新の暗号化ハッシュ値、通帳識別子の抽出
(S4-4)
暗号化ハッシュ値、通帳識別子を銀行公開鍵で暗号化
(S4-5)
暗号化したデータの送信
(S4-6)
(S4-7)
受信データを復号化して、暗号化ハッシュ値、通帳識別子の抽出
(S4-8)
暗号化ハッシュ値を媒体識別子で復号化
(S4-9)
通帳識別子、ハッシュ値の照合
NO
記帳拒否
(S4-10)
YES
(S4-11)
未記帳明細データのハッシュ値の生成

【図１２】


電子通帳登録システム２０
クライアント端末１０
(S4-12)
未記帳明細データ、未記帳明細ハッシュ値を媒体識別子（公開鍵）で暗号化、送信
電子通帳記録媒体に、受信したデータの追加記録
(S4-13)
受信したデータの復号化
(S4-14)
未記帳明細データと未記帳明細ハッシュ値との照合
(S4-15)
電子通帳記録媒体から、多重ハッシュ値の抽出
(S4-16)
多重ハッシュ値及び未記帳明細ハッシュ値から、新しい多重ハッシュ値を生成
(S4-17)
電子通帳記録媒体に、多重ハッシュ値の記録
(S4-18)
記録完了の通知
(S4-19)